

Selling Security to Management

Peter H. Gregory, CISA, CISSP

phg@isecbooks.com

206-779-9711 mobile

About me

- Background in government, finance, non-profit, telecomm, software
 - Published several books on technology & security
 - Speaker at national, regional, local events
 - Interviews in press and trade publications
 - A passion for helping others better understand business risk and how to manage it
-
- And I want to thank the manager I worked for ten years ago... he told me that one day I would become a 'national figure' in this field; little did I know that this would become a reality.

These slides...

- Are available in electronic form:
www.seasim.org
www.isecbooks.com/sim
phg@isecbooks.com

Rules

- This is interactive:
 - this is not about me talking to you – it's about all of us learning more about what works in our respective companies.
- Someone please tell us when we're out of time
- We can continue the dialogue...
 - E-mail
 - Phone
 - Coffee

Problem Statement

Some sort of security is needed. Maybe it's a new firewall, anti-spyware, smart card authentication, encryption on laptops, better role-based access control, or.....

Selling the idea...

- You feel that security is needed in some part of the business. How do you convince management that spending resources on security is a good business decision?

Being sold to...

- One or more persons in the company are trying to convince you that resources should be spent on security. How do you know that this is a good use of company resources?

The reasons...

- Risk analysis dictates that a particular investment is prudent
- Questions:
 - Is the risk analysis thorough and complete?
 - Does the risk analysis accurately depict the risks?
 - Does the risk analysis consider all alternatives?
 - Is the risk analysis technology-focused or business-focused?
 - Given the risks, should the activity be carried out at all? (or, should the asset under threat even *exist*?)
 - What are the consequences of doing nothing?

The reasons...

- Everyone else is doing it
- Questions:
 - WHO else is doing it?
 - WHY are they doing it?
 - SHOULD they be doing it?
 - Are others doing it to compensate for a weakness that you don't have?
 - Did they decide to do it based upon sound business reasoning (like risk analysis), or based upon some less-worthy reason?

The reasons...

- Fear-mongers (aka vendors) say we have to do it, or else...
- Questions:
 - How do they really KNOW that you need it?
 - How do they really know that YOU need it?
 - How can you be sure that the vendor is really just trying to sell us something we may not need?

The reasons...

- We don't want to be the next company that did something stupid
 - (which can be an act of commission or omission)
 - Examples: missing backup tapes, stolen laptops, website break-ins, extortion
- Questions:
 - Have all risks been accurately considered?
 - Are we reacting out of fear, or clear thinking?
 - Could it really happen to us? (and what if it did?)

The reasons...

- It's the law
 - (HIPAA, Sarbanes-Oxley, GLBA, FERC, VISA/PCI*, SB6043, etc.)
- Questions:
 - Do we correctly understand the law's requirements?
 - Are workarounds permitted?
 - What are the consequences of doing nothing?

The reasons...

- It enables / facilitates a business function
 - Examples: centralized authentication, integrated smart cards
- Questions:
 - Has the solution's benefits been qualified and quantified accurately?
 - Has the true cost of implementation been determined?

Also rans...

- “it’s cool” (the technology mantra of the 1990s)
- “it keeps out the bad guys”
- “the hackers won’t get us”

Recap

- The reasons for investing in security solutions:
 - Risk analysis says so
 - Everyone else is doing it
 - Fear-mongers (aka vendors) said so
 - We don't want to read about our company in the headlines
 - It's the law
 - It enables / facilitates a business function
- Recommendation:
 - Adopt a risk management methodology
 - Benefits: consistency, objectivity, accountability
 - Obtain other opinions

Closing thoughts, comments, ideas

Selling Security to Management

Peter H. Gregory, CISA, CISSP

phg@isecbooks.com

206-779-9711 mobile